

The Marine Corps combat team faces diverse challenges stemming from the global war on terrorism ...

for up to 23 different off-base authorities. IIS projects for Camp Pendleton, Camp Lejeune and MCB Quantico are expected to be completed by the end of fiscal year (FY) 2005. The IIS contract to provide identical capabilities for all remaining Marine Corps CONUS installations was awarded in May 2004.

The third immediate effort directed by the MROC is the fielding of E-LMR to Camp Pendleton and MCNCR. The MROC determined that these two sites were exposed to the greatest threat of terrorism and posed the most significant requirement for LMR interoperability. The proposed 30-mile off-base radio coverage delivered by these systems will provide enhanced LMR capabilities. The contract will provide a new trunking system backbone that operates Voice over Internet Protocol (VoIP) allowing follow-on E-LMR expansion and roaming-like capabilities.

Because the E-LMR network adheres to an Association of Public-Safety Communications Officials (APCO) standard (Project 25), it will provide a myriad of interoperability possibilities including system-to-system and over-the-air capabilities that were previously unattainable due to proprietary vendor specifications. The entire backbone infrastructure, including the radios, is fully encrypted with the Advanced Encryption Standard (AES). Although not authorized for classified communications, AES provides a robust encryption capability.

Initially, the new E-LMR environment will provide handheld, vehicular and base station radios to Marine Corps first responders and the location's mission critical requirements, including weapons and test range operations, flight line operations, area guard and other areas that require immediate voice capabilities. The completion of the Camp Pendleton and MCNCR E-LMR systems is scheduled for the first quarter of FY 2006. HQMC has been working on the E-LMR project hand-in-hand with the Navy. Led by the Chief of Naval Installations (CNI) N46, the Navy is moving forward with a similar initiative.

The benefits of E-LMR are many: increased communication that results in increased security for Marine Corps installations, interoperable communications for first responders, which results in dynamic on- and off-base response capabilities and increased safety for operating forces training on range complexes. The cumulative E-LMR benefits and capabilities are dependent on the successful coordination of all the resources that can be aggregated through these wireless communication systems.

The DON proves each day in combat that its capacity to synchronize resources with joint partners enables greater force capabilities over the foe. The value of the improved coordination for first responders will undoubtedly enhance public safety not only on federal installations but also in adjoining communities.

For more information, contact the DON CIO Telecom/Rf Spectrum/Wireless Team at DONSPECTRUMTEAM@navy.mil.

CHIPS



Active Duty Alert Helps Combat Identity Theft

Identity theft is a growing crime in the United States. Consumers, including non-active duty personnel, can take various actions to minimize the risks of identity theft including checking credit reports regularly and keeping track of monthly bills.

Active duty personnel who are away from their regular duty stations are less able to take these steps, so they can be particularly vulnerable to identity theft. To enable personnel on active duty and activated reservists to devote their attention exclusively to the defense needs of the nation, Congress recently created a new tool to help guard against identity theft: the active duty alert.

Active Duty Alert

The active duty alert is a statement that is placed in the credit file of an active duty military consumer so that anyone checking the file for the purpose of establishing or extending credit is informed that the person is on active duty and the identity of the person requesting credit must be verified before the request can be granted.

The active duty alert is part of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amends the Fair Credit Reporting Act (FCRA). Congress designed this alert as a protection for those deployed in locations or situations in which they are unlikely to be able to apply for credit or monitor their financial accounts. *(For more information about FACTA and FCRA, go to http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108 and <http://www.ftc.gov/os/statutes/031224fcra.pdf>, respectively.)*

Under FACTA, if you qualify as an active duty military consumer, you can place an active duty alert in the credit file maintained on you by nationwide consumer reporting agencies. You may also designate a personal representative to place or remove the alert for you. The alert lasts for 12 months, but if you receive an extended deployment, you may place another active duty alert after the first one expires. You may cancel the alert at any time by contacting one of three credit reporting agencies (CRAs): Equifax, Experian and TransUnion. (See the text box on the next page for contact information for the CRAs.)

Credit Reporting Agency (CRA) Contact Information

Equifax P.O. Box 740256 Atlanta, GA 30374 www.equifax.com 1-800-525-6285	Experian P.O. Box 2002 Allen, TX 75013 www.experian.com 1-888-397-3742	TransUnion P.O. Box 1000 Chester, PA 19022 www.transunion.com 1-800-680-7289
--	--	--

To place an active duty alert, you or your personal representative may contact one of the three CRAs, and tell them you want the alert placed in your file. You or your representative will be asked to provide certain personal information as proof of your identity, such as your Social Security Number, name, current address (and most recent previous address if you have been at your current address for less than six months) and other personal information. Be sure to keep this information current for the duration of the alert.

Once you have requested an active duty alert from one of the CRAs, that agency must:

- ✓ Place an alert in your file indicating you are an active duty military member;
- ✓ Remove you from marketing lists for prescreened credit card offers for two years (unless you ask to be placed back on the list before then); and
- ✓ Alert the other two credit reporting agencies through the Fraud Exchange System.

You do not need to contact all three agencies; the CRA that you contact will contact the other two. You will receive confirmation when an alert is added to your credit file.

Once the alert is placed in your credit file, the consumer reporting agencies will notify any business that is asked to establish new credit or extend credit to you about the alert. The business must then take reasonable steps to verify that you are the person seeking credit and not an identity thief.

If you provide a telephone number for verification purposes as part of your active duty alert, the business must try to contact you using that number or take reasonable steps to verify your identity before authorizing any new credit plan or credit extension. The alert may cause some delays if you are trying to obtain credit, but it will also make it more difficult for an identity thief to fraudulently obtain credit in your name.

Credit Protection for All Consumers

Under FACTA, consumers, including non-active duty personnel, can fight identity theft using two other tools: free credit reports and fraud alerts. You can now receive one free credit report from each of the three CRAs each year. Regularly requesting and monitoring your credit report is a good way to control identity theft.

To obtain your free reports, contact the credit reporting agencies or go to <http://www.annualcreditreport.com> for further instructions. Note that free credit reports will be available by region through a nationwide phased rollout starting Dec. 1, 2004, on the West Coast and ending Sept. 1, 2005 on the East Coast. Check the credit report Web site above to determine when people in your state become eligible to receive reports.

If you think you have been a victim of identity theft, you can place a fraud alert in your credit file by contacting any one of the three CRAs. The alert will last for 90 days and requires any creditor to contact you directly before opening any new accounts or changing existing accounts in your name. For further information regarding identity theft, including other steps you can take to minimize the risk of identity theft, visit the Federal Trade Commission (FTC) Web site at <http://www.consumer.gov/idtheft/>.

The FTC has updated its popular booklet "Take Charge: Fighting Back Against Identity Theft," which offers "consumers and businesses meaningful guidance and useful tools for resolving the many different issues facing identity theft victims." The booklet is available from the Web address above.

For information specifically for military and Department of Defense (DoD) personnel, visit the Military Sentinel Web site at <http://www.consumer.gov/military/>. Military Sentinel is a project of the FTC and the DoD to identify and target consumer protection issues that affect members of the U.S. Armed Forces and their families.

At the Military Sentinel Web site, you can enter complaints about suspected fraud attempts and identity theft schemes. To file a consumer complaint, go to the Web site above and click on your service seal. This will link you to the appropriate consumer complaint forms.

Consumer Web sites

Fair and Accurate Credit Transactions Act of 2003 (FACTA)
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108/

Fair Credit Reporting Act (FCRA)
<http://www.ftc.gov/os/statutes/031224fcra.pdf/>

Federal Trade Commission (FTC)
<http://www.consumer.gov/idtheft/>

Military Sentinel
<http://www.consumer.gov/military/>

Patricia Reid Huggins is on the Department of the Navy Chief Information Officer (DON CIO) Information Assurance Team.

Editor's Note: See "Identity Theft," CHIPS Fall 2004 at http://www.chips.navy.mil/archives/04_fall/PDF/identity.pdf and "Identity Theft: A True-Life Crime Story" and "Identity Theft: A Secret Crime," LIFELines at <http://www.lifelines.navy.mil> for more information.

CHIPS